REMARKS

Claims 1-4, 6-16, 33-41 and 45-46 are pending in this application. Claims 1, 16, 33 and 38 are independent claims. Claims 1, 2, 4, 7, 8, 11, 13, 16, 33-36 and 38-41 are amended. Claims 5, 17-32 and 42-44 were previously canceled. Reconsideration and allowance of the present application are respectfully requested.

Claim Rejections under 35 U.S.C. §112

Claims 1-16 and 45 stand rejected under 35 USC §112, first paragraph, as failing to comply with the enablement requirement. This rejection is respectfully traversed.

The Office Action alleged that based on the disclosure of paragraphs 0040-0048 of the present application, digital signatures DS1 and DS2 would never be the same when the private key and public key used in the process are valid keys and the start message is authentic. As is known to one skilled in the art, public key cryptography can be performed by public key encryption and/or digital signatures. In public key encryption, a message encrypted with a recipient's public key can be decrypted only by a possessor of the matching private key. In digital signatures encryption, as disclosed in the present application, a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender had access to the private key, and therefore is likely to be the person associated with the public key. Please see, for example, the attached paper from SearchSecurity.com discussing digital signature. As disclosed in the present application and recited in the pending claims, digital signatures DS1 and DS2 would, in fact, have to match when the private key and public key used in the process are valid keys and the start message is authentic.

Hence, unlike what is alleged in the Office Action, one skilled in the art would understand that digital signatures would have to match for the message to be authenticated. Therefore, Applicant respectfully requests that the rejections of claims 1-16 and 45 under 35 U.S.C. §112 be withdrawn.

Claims 1-16, 33-41 and 45-46 stand rejected under 35 USC §112, first paragraph, as failing to comply with the written description requirement. Claims 1, 16, 33 and 38 have been

amended to overcome the rejection. Therefore, Applicant respectfully requests that the rejections of claims 1-16, 33-41 and 45-46 under 35 U.S.C. §112 be withdrawn.

Claim Rejections under 35 U.S.C. §102

Claims 1, 3, 6, 33, 35, 37-38, 40 and 45-46 stand rejected under 35 U.S.C. §102(b) as being anticipated by Moy ("RFC 2328 – OSPF Version 2") (hereinafter "Moy").

Claims 1, 3-4, 6, 33, 35, 37-38, 40 and 45-46 stand rejected under 35 U.S.C. §102(b) as being anticipated by Murphy et al. ("Digital Signature Protection of the OSPF Routing Protocol") as evidenced by Moy.

Claims 1, 3-4, 6-8, 10-12 and 33, 35-38, 40-41 and 45-46 stand rejected under 35 USC §102(b) as being anticipated by U.S. Patent Publication No. 2002/0016926 to Nguyen et al. (hereinafter "Nguyen et al.") in view of Moy.

These rejections are respectfully traversed.

Moy discloses a specification of the Open Shortest Path First (OSPF) TCP/IP internet routing protocol version 2. OSPF routes IP packets based solely on the destination IP address found in the IP packet header. IP packets are routed "as is" and are not encapsulated in any further protocol headers. Routers use a Hello Protocol to establish and maintain neighbor relationships. Each router sends Hello packets to its neighbors and receives Hello packets from its neighbors. A router periodically advertises its state, also called its linked state. The router's adjacencies are reflected in the contents of its linked state advertisement (LSA). OSPF requires single shot timers which are fired once and cause a protocol event to be processed. OSPF also uses interval timers which are fired at continuous intervals and are used for sending packets at regular intervals. See sections 1, 4, and 9 of Moy. Section 9 of Moy discloses the components of the Interface Data Structure and Section 10.3 of Moy discloses the neighbor state machine.

Applicant submits that Moy does not teach or suggest each of the elements recited in 1, 3, 6, 33, 35, 37-38, 40 and 45-46. Independent claim 1, in part, recites "monitoring a specific multicast channel of a plurality of multicast channels, the specific multicast channel being for sending jump-start messages by a node to other nodes when the node has not received any messages from said other nodes on said specific multicast channel; and sending a jump-start message on said specific multicast channel from a start node that has not received any messages on said specific multicast channel, wherein the jump-start message is secured by the start node

and the start node starts an operation or an application, wherein upon receiving the jump-start message at a receiving node an authenticity of the jump-start message is validated."

Independent claims 33 an 38, in part, recites "send a jump-start message on a specific multicast channel of a system when the node starts an operation or an application and when the node has not received any messages on the specific multicast channel from other nodes, wherein the jump-start message is to be secured by the node." Moy does not teach or suggest at least these features.

There is simply no teaching or suggestion in Moy of a specific multicast channel or a jump-start message, as recited in the pending claims. Moy merely teaches the standard OSPF protocol where Hello packets and LSA are exchanged between routers. The Office Action alleges that the jump start message and the specific channel are inherent features in OSPF routing protocol. As noted above, Moy discloses the complete specification of OSPF version 2. This is no suggestion in this specification, as discloses by Moy, of a specific multicast channel or a jump-start message. One skilled in the art would not conclude that a specific multicast channel and/or a jump-start message are inherent features of the OSPF protocol, as disclosed in Moy, as Moy does not provide any reasons why a specific multicast channel or a jump-start message would be needed and/or used.

None of the cited sections of Moy teaches or suggests "monitoring a specific multicast channel of a plurality of multicast channels, the specific multicast channel being for sending jump-start messages by a node to other nodes when the node has not received any messages from said other nodes on said specific multicast channel," as recited in the pending claims. There is also no teaching or suggest in Moy of "sending a jump-start message on said specific multicast channel from a start node that has not received any messages on said specific multicast channel, wherein the jump-start message is secured by the start node and the start node starts an operation or an application," as recited in the pending claims. Moy also does not teach or suggest "upon receiving the jump-start message at a receiving node an authenticity of the jump-start message is validated."

As noted in the Office Action, Murphy and Nguyen do not teach or suggest "sending a jump-start message on said specific multicast channel from a start node that has not received any messages on said specific multicast channel, wherein the jump-start message is secured by the

start node and the start node starts an operation or an application." Therefore, Murphy and Nguyen do not cure any of the deficiencies of Moy.

Based on the distinctions noted above, Applicant submits that Moy, Murphy and/or Nguyen do not teach or suggest each of the elements recited in claims 1, 33 and 38. Each of claims 2-4, 6-15, 34-27, 39-41 and 45-46 depend on claims 1, 33 and 38 and therefore incorporates all of the elements of claims 1, 33 and 38, in addition to the further elements recited in claims 2-4, 6-15, 34-27, 39-41 and 45-46. Hence, claims 2-4, 6-15, 34-27, 39-41 and 45-46 are allow allowable at least because of their dependence on claims 1, 33 and 38. Therefore, Applicant respectfully requests that this rejection of claims 1, 3-4, 6, 33, 35, 37-38, 40-41 and 45-46 under 35 U.S.C. §102 be withdrawn.

Claim Rejections Under 35 U.S.C. §103

Claims 2, 34 and 39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moy as applied to claims 1, 33 and 38. Claims 2, 34 and 39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Murphy in view of Moy as applied to claims 1, 33 and 38. Claims 2, 34 and 39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen in view of Moy as applied to claims 1, 33 and 38. Claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen in view of Moy as applied to claim 7 and further in view of U.S. Patent No. 6,085,320 to Kaliski, Jr. (hereinafter "Kaliski"). Claims 13-15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen in view of Moy as applied to claim 1 and further in view of U.S. Patent No. 7,103,185 to Srivastava et al. (hereinafter "Srivastava"). These rejections are respectfully traversed.

None of the cited references teach or suggest "monitoring a specific multicast channel of a plurality of multicast channels, the specific multicast channel being for sending jump-start messages by a node to other nodes when the node has not received any messages from said other nodes on said specific multicast channel," as recited in the pending claims. None of the cited references teach or suggest "sending a jump-start message on said specific multicast channel from a start node that has not received any messages on said specific multicast channel, wherein the jump-start message is secured by the start node and the start node starts an operation or an application," as recited in the pending claims. None of the cited references teach or suggest "upon receiving the jump-start message at a receiving node an authenticity of the jump-start

message is validated." In order words, none of the cited references cures any of the deficiencies of Moy, as outlined above. Therefore, Applicant respectfully requests that the rejections of claims 2, 9, 13-15, 34, 35 and 39 under 35 U.S.C. §103 be withdrawn.

Allowable Subject Matter

Applicant notes with appreciation the Examiner's indication that claim 16 would be allowable over the prior art of record, subject to the 112, 1st paragraph rejections. Claim 16 has been amended to overcome the rejection. Based on the amendments to the pending claims and the arguments presented above, Applicant respectfully requests that claim 16, and the other pending claims, be allowed and that this application be passed to issue.

Disclaimer

Applicant may not have presented all possible arguments or have refuted the characterizations of either the claims or the prior art as found in the Office Action. However, the lack of such arguments or refutations is not intended to act as a waiver of such arguments or as concurrence with such characterizations.

CONCLUSION

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

The Office is authorized to charge any necessary fees to Deposit Account No. 22-0185.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 27592-00454-US from which the undersigned is authorized to draw.

Dated: April 9, 2009

Respectfully submitted,

Electronic signature: /Arlene P. Neal/
Arlene P. Neal
Registration No.: 43,828
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant

Enclosures: Digital Signatures
SearchSecurity.com Definitions

ATTACHMENT

SearchSecurity.com Definitions (Powered by Whatis.com)

LOOK UP TECH TERMS Powered by:

Search listings for thousands of IT terms: SEARCH

Browse tech terms alphabetically:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z #

digital signature

DEFINITION - A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

How It Works

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the contract (it's a short one!) into an e-mail

note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.
3. If the hashes match, the received message is valid.

Also see hashing and Digital Signature Standard.

Getting started with digital signatures

To explore how **digital signatures** are used in the enterprise, here are some additional resources:

Personal digital certificate pros and cons: Are you considering creating a personal digital certificate for your company? Learn about the pros and cons of the technology and the proper steps to follow for issuing these certificates.

Understanding multifactor authentication features in IAM suites: Do you think your organization's multifactor authentication strategy works effectively with your IAM suite? Get a better understanding of multifactor authentication, your IAM suite options and best practices for deployment.

LAST UPDATED: 05 Oct 2008

Read more about digital signature:

- The American Bar Association provides guidelines for the use of digital signatures.
- The World Wide Web Consortium (W3C) describes its own Digital Signature Initiative.
- SearchSecurity.com provides links to more information about digital signatures.
- SearchCRM.com has information about the use of digital signatures in customer relationship management.

Do you have something to add to this definition? Let us know.
Send your comments to techterms@whatis.com

Digg This! StumbleUpon Del.icio.us

SECURITY RELATED LINKS

Ads by Google

PDF Digital Signatures
Sign, Validate, Certify PDF documents. Download trial.